IN THE CLAIMS

Please amend the claims as indicated in the rewritten claims listed below:

Claim Amendments:

1-29. (canceled)

30. (Currently Amended) A method for using a security apparatus to provide security for a computer system, comprising:

dynamically loading into the security apparatus information permitting detection of vulnerabilities and exposures for an application and information on how the security apparatus is to prevent exploitation of the vulnerabilities and exposures on the computer system;

using the security apparatus to intercept data traffic entering the computer system; ~~and~~

using the dynamically loaded information to process the intercepted data to prevent exploitation of the vulnerabilities and exposures on the computer system, wherein the security apparatus uses new information on vulnerabilities and exposures to handle new application sessions for the application and uses old information on vulnerabilities and exposures to handle existing application sessions for the application;

<u>maintaining a list of which information elements are used by the vulnerabilities and exposures; and</u>

<u>during processing of the data traffic, decoding only the information elements in the data traffic that appear in the list.</u>

31. (Canceled)

32. (Previously Presented) The method defined in claim 30 further comprising:

performing transport layer functions including selectively intercepting data traffic, and dropping, forwarding, and bypassing some of the data traffic.

33. (Previously Presented) The method defined in claim 30 further comprising:

using virtual patches and decoder plug-ins to create an interpreter configuration data structure; and

using the interpreter configuration data structure at the security apparatus to process the intercepted

data to prevent exploitation of the vulnerabilities and exposures in the computer system.

34. (Previously Presented) The method defined in claim 30 wherein there are multiple applications that run on the computer system and wherein information on vulnerabilities and exposures for each of the multiple applications is dynamically loaded into the security apparatus, the method further comprising:

using virtual proxies on the security apparatus to process the intercepted data based on the dynamically-loaded information, wherein there is a separate virtual proxy for each of the applications on the computer system.

35. (Previously Presented) The method defined in claim 30 wherein the data traffic includes information elements, the method further comprising:

using virtual proxies on the security apparatus to drop at least some of the information elements in the data traffic.

36. (Previously Presented) The method defined in claim 30 wherein the data traffic includes information elements, the method further comprising:

using virtual proxies on the security apparatus to modify at least some of the information elements in the data traffic.

37. (Previously Presented) The method defined in claim 30 wherein the data traffic includes information elements, the method further comprising:

using virtual proxies on the security apparatus to insert new information elements into the data traffic.

38. (Previously Presented) The method defined in claim 30 wherein the data traffic includes information elements of various types, wherein the dynamically-loaded information comprises a tree that contains a static element corresponding to each type of information element, and wherein each static element contains a list of processing procedures for the vulnerabilities and exposures and contains a list of decoding procedures for decoding children of the information

elements, the method further comprising triggering the processing and decoding procedures for each information element using the static element corresponding to that information element.

39. (Previously Presented) The method defined in claim 38, further comprising:

using the static elements in determining whether to pass the information elements.

40. (Previously Presented) The method defined in claim 38, further comprising:

using the static elements in determining whether to flush the information elements.

41. (Previously Presented) The method defined in claim 38, further comprising:

using the static elements in determining whether to load the information elements.

42. (Previously Presented) The method defined in claim 30 further comprising:

converting information about the vulnerabilities and exposures into an intermediate form that is loaded into the security apparatus as the dynamically-loaded information and that optimizes processing speed for the processing of the intercepted data to prevent exploitation of the vulnerabilities and exposures on the computer system; and

identifying information elements that are needed for processing the vulnerabilities and exposures and inserting this information into the intermediate form.

43. (Previously Presented) The method defined in claim 30 further comprising:

converting information about the vulnerabilities and exposures into an intermediate form that is loaded into the security apparatus as the dynamically-loaded information and that optimizes processing speed for the processing of the intercepted data to prevent exploitation of the vulnerabilities and exposures on the computer system; and

identifying when to load, flush, and pass information elements in the data traffic to minimize latency and inserting this information into the intermediate form.

44. (Previously Presented) The method defined in claim 30 further comprising:

converting information about the vulnerabilities and exposures into an intermediate form that is loaded into the security apparatus as the dynamically-loaded information and that optimizes processing speed for the processing of the intercepted data to prevent exploitation of the vulnerabilities and exposures on the computer system; and

extracting regular expression matches, pattern matches, and value list comparisons from the information about the vulnerabilities and exposures and converting the matches and comparisons into the intermediate form to optimize the processing of the intercepted data.